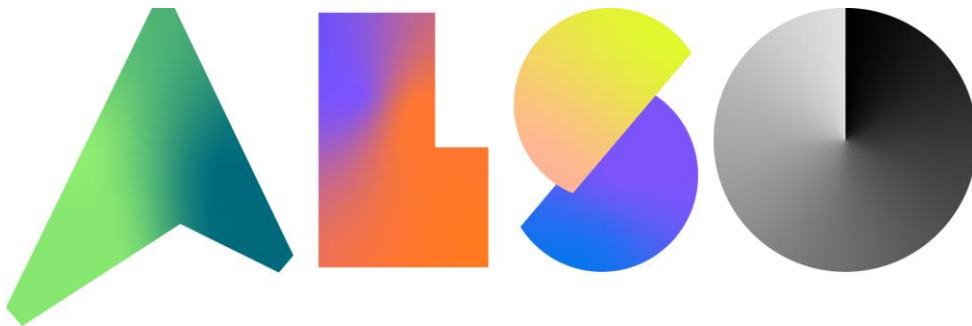


How to Fortinet

Konfiguration eines IPsec VPN-Tunnel zwischen einer FortiGate und Sophos UTM Firewall

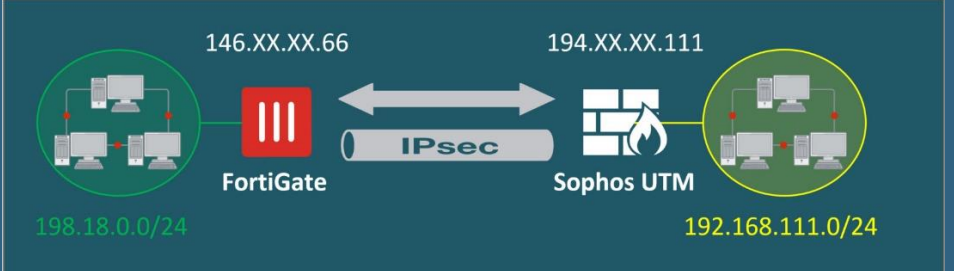


Inhaltsverzeichnis

AUSGANGSLAGE	3
KONFIGURATION AUF DER FORTIGATE 300D	4
Konfigurieren des VPN Tunnels über das Webgui:	4
Netzwerkeinstellungen:.....	4
Authentication konfigurieren:	4
Phase 1 Parameter konfigurieren:	5
Phase 2 Selektoren konfigurieren:	5
Konfigurieren der Routen:	6
Konfigurieren der Policies:.....	7
Konfigurieren des VPN Tunnels über die CLI:	8
VPN Phase 1 konfigurieren:	8
VPN Phase 2 konfigurieren:	8
Routen konfigurieren:.....	8
Adress Objekte für Policies konfigurieren:	8
Policy konfigurieren:.....	9
KONFIGURATION AUF DER SOPHOS UTM	10
Neuen Tunnel erstellen:	10
Remote Gateway:	11
Policy:	12
Connections:	13
ERFOLGSKONTROLLE :	14
VPN Monitor auf der FortiGate :	14
VPN Monitor auf der Sophos UTM Firewall:	14

Ausgangslage

In diesem Dokument wird beschrieben, wie ein Site to Site VPN zwischen einer FortiGate und einer Sophos UTM Firewall konfiguriert werden kann. Dieses Setup wurde unter folgenden Bedingungen aufgebaut und durchgetestet:

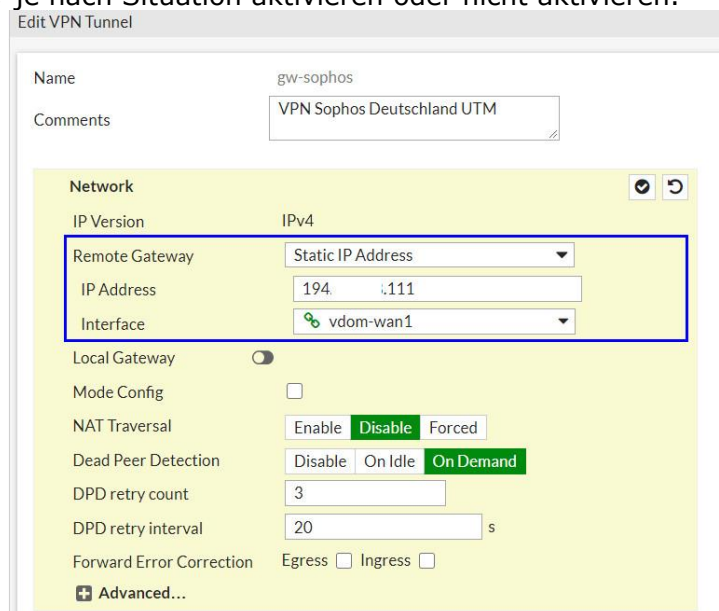
	Seite FortiGate	Seite Sophos UTM
Netzplan		
Hardware	FortiGate 300D	Sophos UTM/SG
Software	4.6.2 build1723	V9.703-3
Lokales Netzwerk	198.18.0.0/24	192.168.111.0/24
Public IP Adresse	146.XX.XX.66	194.XX.XX.111
Authentication	Pre-shared Key definieren	
IKE Version	Version 1 (Die UTM unterstützt IKE Version 2 nicht)	
Phase 1 Proposal	Alogrithms: AES256-SHA256 DH-Group 5	
Phase 1 Key Lifetime	86400 Sekunden	
Phase 2 Proposal	Alogrithms: AES256-SHA512 / PFS-DH-Group 5	
Phase 2 key Lifetime	43200 Sekunden	

Konfiguration auf der FortiGate 300D

Konfigurieren des VPN Tunnels über das Webgui:

Netzwerkeinstellungen:

1. VPN Tunnel Name definieren. (Mit diesem Namen wird beim WAN Interface das Tunnelinterface gebildet.)
2. Bei Remote Gateway den Typ auf *Static IP Address* stellen.
3. Im Feld *IP Address* wird die Public IP-Adresse der Sophos UTM Firewall eingetragen (194.XX.XX.111)
4. Bei *Interface* wird das ausgehende Interface (meistens WAN) angegeben. Auf diesem Interface wird das Tunnelinterface dann als Subinterface gebildet.
5. *NAT Traversal*: je nach Situation aktivieren oder nicht aktivieren.



Edit VPN Tunnel

Name: gw-sophos

Comments: VPN Sophos Deutschland UTM

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 194.XX.XX.111

Interface: vdom-wan1

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: Enable **Disable** Forced

Dead Peer Detection: Disable On Idle **On Demand**

DPD retry count: 3

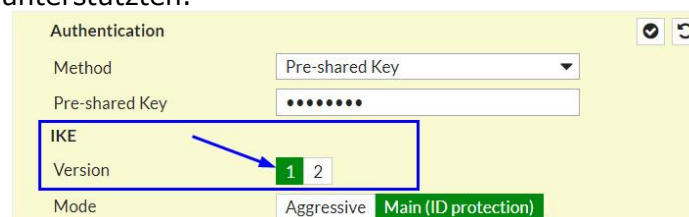
DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

Authentication konfigurieren:

1. *Method* Auf Pre-shared Key einstellen.
2. Im Feld *Pre-shared Key* einen komplexen, nicht nachvollziehbaren Key konfigurieren (dieser Key wird auf der Checkpoint dann auch benötigt)
3. Wir müssen die *IKE* Version 1 auswählen, da die Sophos UTM Modelle den Standard IKE Version 2 nicht unterstützen.



Authentication

Method: Pre-shared Key

Pre-shared Key:

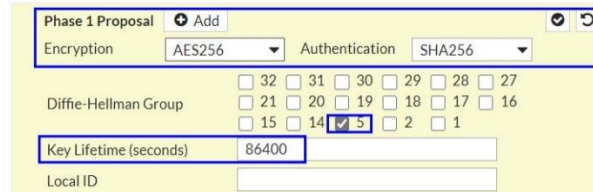
IKE

Version: **1** 2

Mode: Aggressive **Main (ID protection)**

Phase 1 Parameter konfigurieren:

1. Encryption auf AES256 und Authentication auf SHA256 konfigurieren.
2. Alle anderen Encryption und Authentications Parameter entfernen.
3. Die Diffie-Hellman Group wird auf 5 eingestellt.
4. Der Parameter Key Lifetime (seconds) auf 86400 (1440 Minuten) stellen. (Dies muss unbedingt mit der Gegenseite gleich definiert werden)

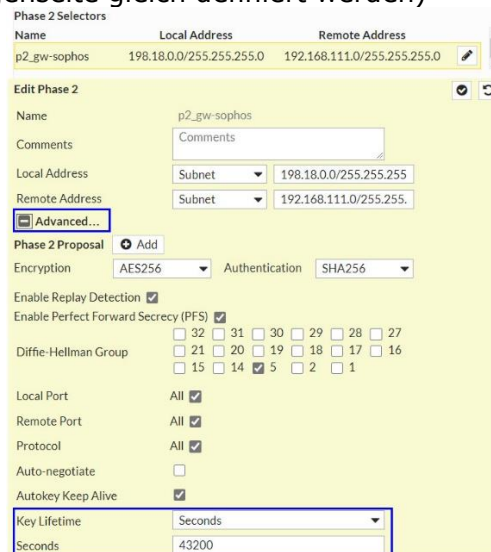


Phase 2 Selektoren konfigurieren:

Auf der Sophos wird der Term 0.0.0.0/0 nicht unterstützt.

In unserem Beispiel wird Local 198.18.0.0/24 und Remote Netz 192.168.111.0/24 konfiguriert.

1. Name in diesem Feld kann ein Name für den Selektor definiert werden (Übersicht wahren)
2. Local Address Das Netz welches bei der Fortigate erreicht werden soll. Typ auf Subnet stellen und Adresse: 198.18.0.0/24 konfigurieren.
3. Remote Address Das Netz welches wir hinter der Sophos UTM Firewall erreichen wollen. Typ auf Subnet stellen und Adresse 192.168.111.0/24 konfigurieren.
4. Unter dem Menüpunkt Advanced können die Phase 2 Proposal konfiguriert werden.
5. Encryption auf AES256 und Authentication auf SHA256 stellen. Alle anderen Encryption und Authentications Parameter entfernen. (Auf das X klicken)
6. Perfect Forward Secrecy (PFS) aktivieren
7. Die Diffie-Hellman Group auf 14 einstellen.
8. Key Lifetime auf Second stellen und dann 43200 Sekunden einstellen (Dies muss unbedingt mit der Gegenseite gleich definiert werden)

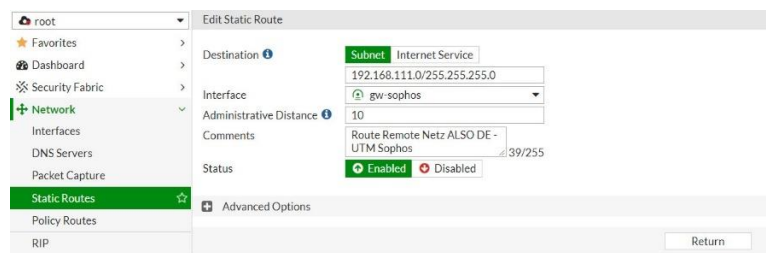


Konfigurieren der Routen:

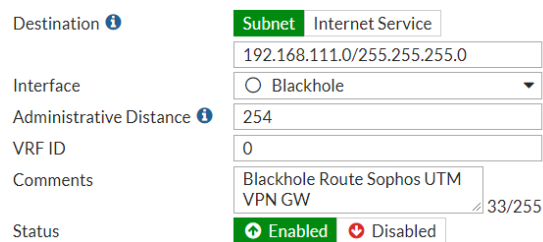
Auf der FortiGate müssen die Netze der Remote Seite in den IPSec Tunnel geroutet werden. Dabei zeigt die Route auf das Tunnelinterface (gw-sophos). Damit bei einem Unterbruch des Tunnels, der Traffic nicht über die Default Route ins Internet geroutet wird, sollte eine Blackhole Route konfiguriert werden.

Die Routen werden folgendermassen konfiguriert: Menu: *Network* → *Static Routes* → 

Route Remote Netz:




Blackhole Route:

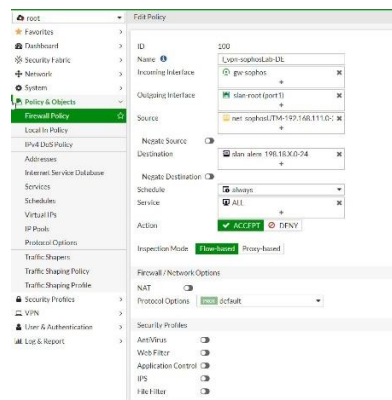


Konfigurieren der Policies:

Es braucht mindestens eine Policy auf der FortiGate. Damit der Traffic bi-direktional durch den Tunnel geht, empfiehlt es sich eine Regel in jede Richtung zu konfigurieren. Dabei ist die Kommunikation zwischen dem vpn Tunnel Interface (gw-sophos) und dem internen Interface (port1).

Menu : *Policy & Objects* → *IPv4 Policy* → 

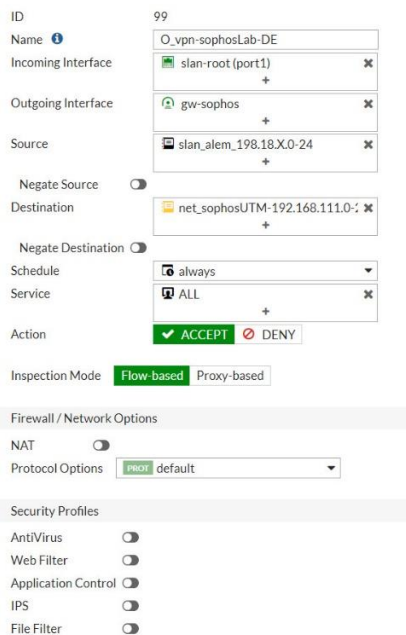
Policy 1 : Zugriff 192.168.111.0/24 → 198.18.0.0/24



Policy configuration details for Policy 1:

- ID:** 200
- Name:** O_vpn-sophosLab-DE
- Incoming Interface:** gw-sophos
- Outgoing Interface:** slsn-root (port1)
- Source:** net_sophosUTM-192.168.111.0/24
- Negate Source:** ☐
- Destination:** slsn_alen_198.18.X.0-24
- Negate Destination:** ☐
- Schedule:** always
- Service:** ALL
- Action:** ☒ ACCEPT ☐ DENY
- Inspection Mode:** Flow-based
- Firewall / Network Options:**
 - NAT:** ☐
 - Protocol Options:** default
- Security Profiles:**
 - AntiVirus: ☐
 - Web Filter: ☐
 - Application Control: ☐
 - IPS: ☐
 - File Filter: ☐

Policy 2 : Zugriff 198.18.0.0/24 → 192.168.111.0/24



Policy configuration details for Policy 2:

- ID:** 99
- Name:** O_vpn-sophosLab-DE
- Incoming Interface:** slsn-root (port1)
- Outgoing Interface:** gw-sophos
- Source:** slsn_alen_198.18.X.0-24
- Negate Source:** ☐
- Destination:** net_sophosUTM-192.168.111.0/24
- Negate Destination:** ☐
- Schedule:** always
- Service:** ALL
- Action:** ☒ ACCEPT ☐ DENY
- Inspection Mode:** Flow-based
- Firewall / Network Options:**
 - NAT:** ☐
 - Protocol Options:** default
- Security Profiles:**
 - AntiVirus: ☐
 - Web Filter: ☐
 - Application Control: ☐
 - IPS: ☐
 - File Filter: ☐

Regelset :

-- Allow S2S VPN ALSO-CH Lab to ALSO-DE LAB -- 2/2									
O_vpn-sophosLab-DE	slan-root (port1)	gw-sophos	slan_alen_198.18.X.0-24	net_sophosUTM-192.168.111.0-24	always	ALL	ACCEPT	Disabled	
I_vpn-sophosLab-DE	gw-sophos	slan-root (port1)	net_sophosUTM-192.168.111.0-24	slan_alen_198.18.X.0-24	always	ALL	ACCEPT	Disabled	

Konfigurieren des VPN Tunnels über die CLI:

VPN Phase 1 konfigurieren:

```
config vpn ipsec phase1-interface
    edit "[VPN_NAME]"
        set interface "[WAN-INTERFACE]"
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set comments "VPN zu Sophos UTM"
        set dhgrp 5
        set nattraversal disable
        set remote-gw [PUBLIC_IP_SOPHOS-UTM]
        set psksecret [PRESHARED-KEY]
    next
end
```

VPN Phase 2 konfigurieren:

```
config vpn ipsec phase2-interface
    edit "p2_[VPN_NAME]"
        set phase1name "[VPN_NAME]"
        set proposal aes256-sha256
        set dhgrp 5
        set keepalive enable
        set src-subnet [MEIN_LOKALES_NETZWERK NETZMASKE]
        set dst-subnet [REMOTE_NETZWERK_NETZMASKE]
    next
end
```

Routen konfigurieren:

```
config router static
    edit 2
        set dst [REMOTE_NETZWERK_NETZMASKE]
        set device "[VPN_NAME]"
        set comment "Route Remote Netz ALSO DE - UTM Sophos "
    next
    edit 3
        set dst [REMOTE_NETZWERK_NETZMASKE]
        set comment "Blackhole [REMOTE_NETZWERK_NETZMASKE]"
        set distance 254
        set blackhole enable
    next
end
```

Adress Objekte für Policies konfigurieren:

```
config firewall address
    edit "[NAME_ADRESSOBJEKT_REMOTE_NETZWERK]"
        set color 10
        set subnet [NETZWERK_ADRESSE] [SUBNETZMASKE]
    next
    edit "[NAME_ADRESSOBJEKT_INTERNES_NETZWERK]"
        set color 10
        set subnet [NETZWERK_ADRESSE] [SUBNETZMASKE]
    next
end
```


Policy konfigurieren:

```
config firewall policy
  edit 1
    set name "O_vpn-sophosUTM"
    set srcintf "[INTERNES_INTERFACE]"
    set dstintf "[VPN_NAME]"
    set srcaddr "[NAME_ADRESSOBJEKT_INTERNES_NETZWERK]"
    set dstaddr "[NAME_ADRESSOBJEKT_REMOTE_NETZWERK]"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
  edit 2
    set name "I_vpn-sophosUTM"
    set srcintf "[VPN_NAME]"
    set dstintf "[INTERNES_INTERFACE]"
    set srcaddr "[NAME_ADRESSOBJEKT_REMOTE_NETZWERK]"
    set dstaddr "[NAME_ADRESSOBJEKT_INTERNES_NETZWERK]"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
end
```

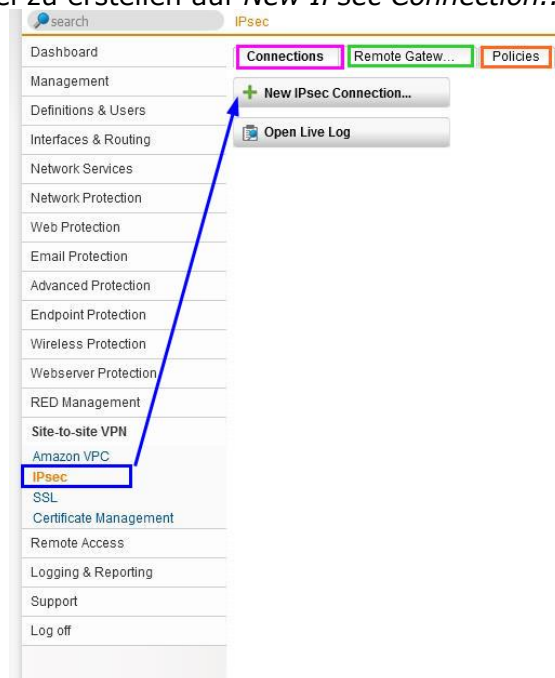
Konfiguration auf der Sophos UTM

Auf der Sophos UTM Firewall wird ein VPN folgendermassen aufgebaut:

- **Connections:** Hier wird der Lokale Teil konfiguriert. Das Lokale Netzwerk, das Interface welches als Listener definiert wird (meistens ein WAN Interface)
- **Remote Gateway:** In diesem Abschnitt werden die Remote VPN Gateway Parameter konfiguriert. In unserem Fall ist dies die Public IP Adresse der FortiGate und das Remote Netzwerk welches wir hinter der FortiGate erreichen wollen.
- **Policy:** werden die Verschlüsselung Parameter konfiguriert.

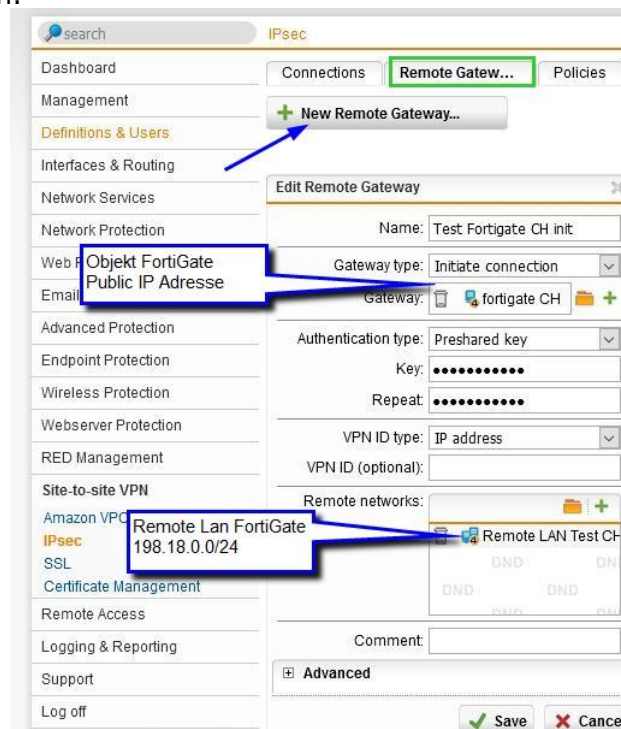
Neuen Tunnel erstellen:

1. Unter dem Menu *Site-to-site VPN* auf *IPsec*
2. Um den neuen Tunnel zu erstellen auf *New IPsec Connection...* klicken.



Remote Gateway:

1. Name definieren im Feld *Name*
2. *Gateway type* wie soll sich der Tunnel aufbauen (Sophos UTM als initiator oder als Responder) konfigurieren. Wir haben beide Varianten ausprobiert. Beide funktionieren ohne, dass auf der FortiGate was verändert werden muss.
3. *Authentication type* haben wir mit einem Preshared Key konfiguriert. Dieser muss natürlich auf der FortiGate deckungsgleich eingegeben werden.
4. *VPN ID type* soll auf *IP address* gelassen werden. (Die FortiGate interpretiert die IP-Adresse der Sophos UTM als ID)
5. Im Feld *Remote networks* werden die Netze auf der Gegenseite definiert, welche aus dem Sophos Netzwerk erreicht werden sollen.
 ! Die Sophos unterstützt 0.0.0.0/0 nicht (Was auch gut so ist).
 Über das Icon + kann ein neues Remote Netzwerk Objekt erstellt werden.
6. Alles abspeichern und dann kann das erstellte Remote Gateway Profil unter Connections ausgewählt werden.



Search IPsec

Dashboard Connections **Remote Gateway...** Policies

Management

Definitions & Users **+ New Remote Gateway...**

Interfaces & Routing

Network Services

Network Protection

Web Filter

Email

Advanced Protection

Endpoint Protection

Wireless Protection

Webserver Protection

RED Management

Site-to-site VPN

Amazon VPC

IPsec

SSL

Certificate Management

Remote Access

Logging & Reporting

Support

Log off

Edit Remote Gateway

Name: Test Fortigate CH init

Gateway type: Initiate connection

Gateway: fortigate CH

Authentication type: Preshared key

Key:

Repeat:

VPN ID type: IP address

VPN ID (optional):

Remote networks:

Remote Lan FortiGate 198.18.0.0/24

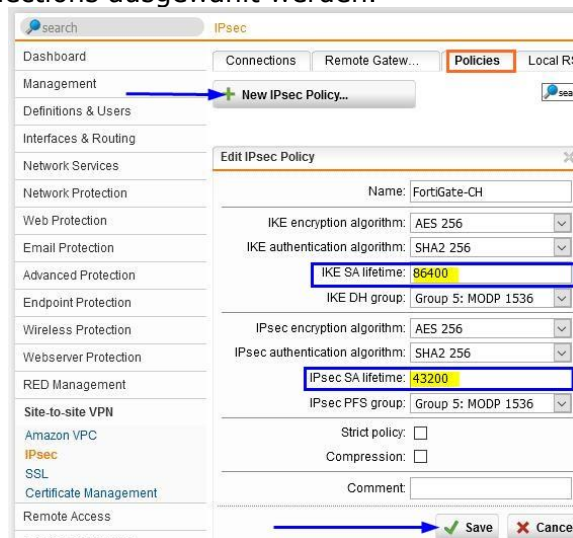
Comment:

Advanced

Save Cancel

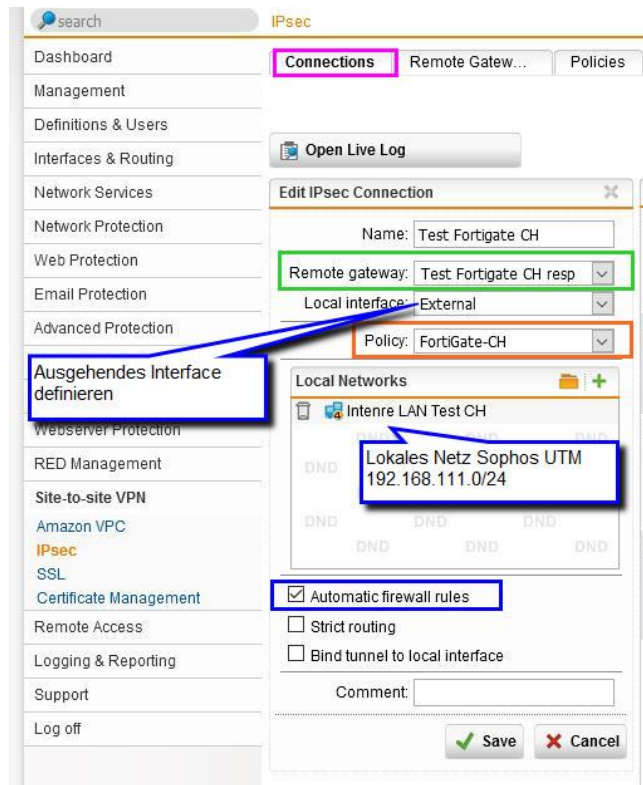
Policy:

1. unter Sophos-utm-newObject.jpgg new IPsec Policy kann eine neue VPN Policy konfiguriert werden.
2. Name In diesem Feld wird tatsächlich der Name der Policy angegeben. (Policy hat auf der Sophos eine andere Bedeutung wie auf der FortiGate)
3. Die entsprechenden Phase 1 und Phase 2 Parameter deckungsgleich wie auf der FortiGate definieren. Achtung die FortiGate und die Sophos UTM haben nicht dieselben default Life Time in den entsprechenden Phasen. diese sind unbedingt aufeinander abzugleichen.
4. Mit dem Button Save wird die neue Policy mit dem definierten Namen erstellt und kann dann im Menu 'Connections ausgewählt werden.



Connections:

1. Im Connections Menu jetzt die angelegten Profile auswählen:
2. *Remote Gateway* das vorher konfigurierte Profil aus Remote Gateway anwählen
3. unter Policy die VPN Policy auswählen, welche vorher definiert wurde
4. *Local interface* Hier wird definiert auf welchem Interface der VPN Tunnel auf der Sophos terminiert (in unserem Fall External)
5. Lokale Netzwerke auswählen, welche für das VPN vorgesehen sind
6. die Option *Automatic firewall rules* aktivieren, damit die Sophos beim speichern automatisch die Firewall Regeln gemäss VPN Definition erstellt im Regelwerk.
7. Mit *Save* den IPSec Tunnel erstellen und dann testen.



The screenshot displays the Fortinet FortiGate web interface for configuring an IPsec connection. The left sidebar shows the navigation menu with 'Connections' highlighted. The main panel shows the 'Edit IPsec Connection' window. Key configuration details include:

- Name:** Test Fortigate CH
- Remote gateway:** Test Fortigate CH resp (highlighted with a green box)
- Local interface:** External (highlighted with a blue box and a callout 'Ausgehendes Interface definieren')
- Policy:** FortiGate-CH (highlighted with an orange box)
- Local Networks:** Includes 'Interne LAN Test CH' and 'Lokales Netz Sophos UTM 192.168.111.0/24' (highlighted with a blue box).
- Automatic firewall rules:** Checked (highlighted with a blue box).
- Other options:** Strict routing and Bind tunnel to local interface are unchecked.
- Buttons:** Save and Cancel buttons are at the bottom right.

Erfolgskontrolle :

VPN Monitor auf der FortiGate :

FortiGate 300D alsochlu-sg0e1 HA: Primary admin				
root	View	Search		
Tunnel	Interface Binding	Status	Ref.	
Custom				
alsoLab-	vdom-wan1	Up	7	
gw-sophos	vdom-wan1	Up	4	
gw-sophosXG	vdom-wan1	Inactive	4	
Dialup - FortiClient (Windows, Mac OS, Android)				
lab-also	vdom-wan1	Inactive	1	

VPN Monitor auf der Sophos UTM Firewall:

Test Fortigate CH [1 of 1 IPsec SAs established]

SA: 192.168.111.0/24=194. .111 146. .66=198.18.0.0/24

VPN ID: 194. .111

IKE: Auth PSK / Enc AES_CBC_256 / Hash HMAC_SHA2_256 / Lifetime 86400s / PFS MODP_1536 / DPD

ESP: Enc AES_CBC_256 / Hash HMAC_SHA2_256_128 / Lifetime 43200s

Phase 1 Up

Phase 2 Up